

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



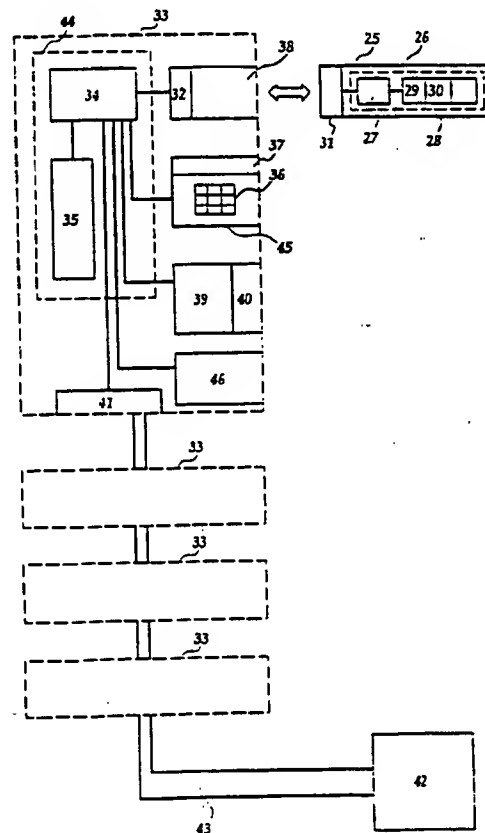
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G07C 9/00, G07F 7/10		A1	(11) International Publication Number: WO 94/10658
			(43) International Publication Date: 11 May 1994 (11.05.94)
(21) International Application Number: PCT/AU93/00576 (22) International Filing Date: 5 November 1993 (05.11.93) (30) Priority data: PL 5700 5 November 1992 (05.11.92) AU (71) Applicant (for all designated States except US): COMS21 PTY. LTD. [AU/AU]; 52 Hoskins Street, Mitchell, ACT 2911 (AU). (72) Inventor; and (75) Inventor/Applicant (for US only) : GREEN, Graeme, Allan [AU/AU]; 52 Hoskins Street, Mitchell, ACT 2911 (AU). (74) Agent: RAINEY, David; Thomson Pizzey, P.O. Box 291, Woden, ACT 2606 (AU).		(81) Designated States: AT, AU, BB, BG, BR, BY, CA, CH, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, LV, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Published With international search report.	

(54) Title: **SECURE ACCESS CONTROL SYSTEM**

(57) Abstract

A secure access control system has a "smart" key assembly (25) with storage means (28) for storing identification data (29) and image data (30). An interface (31) provides communication between the key assembly (25) and an access control assembly (33) having a data processing assembly (44), a user interface assembly (45), a receiving slot (38) for the key assembly (25) and an identity verifier (39). The data processing assembly (44) is controlled by a central processor (34) and has data storage means (35). The user interface assembly has a keypad (36) and an LCD (37). The identity verifier (39) compares a sensed identification of a user with the image data (30) embedded in the key assembly (25).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

"SECURE ACCESS CONTROL SYSTEM"BACKGROUND OF INVENTION

5 This invention relates to a secure access control system.

The invention has particular but not exclusive application to a secure access control system for use in gaming establishments such as casinos and for illustrative purposes reference will be made herein to
10 such an application. However it is to be understood that this invention can be used in many other applications, such as for example restricted area security, automatic teller machines, medical records, information retrieval etc, where control of access to only authorised users is
15 important.

DESCRIPTION OF THE PRIOR ART

Secure access control systems are well known. It is known to provide mechanical and electronic locks or
20 access barriers which are "releasable" when a personal identification number (PIN) is entered on a keypad by a user or when operated by use of an encoded card or key.

It is known to use such cards in conjunction with a PIN to provide access only to authorised users who can
25 enter the correct PIN. These known secure access systems provide access to remote sites and are controlled by a centralised computer system. However if the centralised computer is inoperable at any time, the remote site facility is also inoperable.

30 It is also known to provide identification cards or security access devices which include memory and circuitry enabling the memory to be read from, written to or otherwise modified. Such cards can include electrically erasable programmable read only memory
35 (EEPROM) and are known in the art as "smartcards". Such devices are disclosed in US patents 4675516, 4725924, 4727246, 4733061 and 4764666.

The use of coin actuated gaming and amusement

machines is well known. The administrative, labour and logistical problems associated with the management of the very large coin or token holdings in casinos and fun parlours has led to a requirement for gaming machines which are "cashless" in the sense that they are operated by a card or other device whereby the gaming machine is coin-freed. Australian patents 511904 and 613484 and Australian patent application 72657/91 illustrate such "cashless" equipment. The latter two disclose the use of smart cards such as those described above.

The management and audit functions in casinos and fun or amusement parlours is complex because of the large turnover, the large number of machines and the vast quantity of statistical information available for analysis. These functions may be performed manually by collating data manually extracted from each individual machine. However it is now not uncommon for this function to be carried out electronically either by a centralised computer facility connected to individual machines by a landline as exemplified in Australian patent 542455 and Australian patent application 72657/91, or by on-site down-loading from individual machines to a transportable data collector as exemplified in Australian patents 553309 and 613484. However failure of the central computer in systems using landlines can render individual machines inoperative. Furthermore in systems using on-site down-loading, security at individual machines can be compromised by the lack of a centralised control as this cannot be provided in the absence of on-line real time data.

SUMMARY OF THE INVENTION

The present invention aims to provide a useful alternative to known secure access control systems which will be reliable and efficient in use.

This invention in one aspect resides broadly in a secure access control system including:-

at least one key assembly having a data processing

assembly including processor means and data storage means for receiving identification data relevant to a user of the system;

5 a plurality of access control assemblies adapted to receive a key assembly, each access control assembly having a data processing assembly including processor means and data storage means, and

interface means whereby an access control assembly can communicate with a received key assembly.

10 As used herein the expression "key assembly" includes devices for permitting access by a user to a secure access system upon correct use of the device by the user. Cards and keys are examples of key assemblies. The secure access control system may include a central
15 computer assembly, and communication means for transferring data from the access control assemblies to the central computer assembly.

In a preferred embodiment the access control assemblies include a user interface assembly operable by
20 a user to input data to the access control assembly.

The user interface assembly can include any suitable means whereby the user is able to communicate with the access control assembly and it is preferred that the user interface assembly includes input means and information
25 display means.

The input means could be a joy-stick or a mouse or a screen-based electronic pencil. Alternatively the input means can be a microphone for recording the voice instructions of a user. However it is preferred that the
30 input means includes a keypad.

In a preferred embodiment the access control assembly includes receiving means for closely receiving and releasably retaining a key assembly whereby communication is established between the access control
35 assembly and the key assembly by the interface means.

An access control assembly may verify a user's identification by comparing a PIN entered by the user with a PIN stored in the key assembly data storage means.

However it is preferred that each access control assembly has identity verification means for verifying identification data stored in the key assembly data storage means. Thus the identity verification means may
5 include sensing means for sensing personal physical characteristics of a user.

The sensing means may sense a range of personal physical characteristics. Thus the sensing means may sense skin print images or finger prints as described in
10 Australian patent applications 87582/91 and 67230/90, or finger profiles as described in Australian patent application 55243/90. Alternatively the sensing means may sense voice tones. However it is preferred that the sensing means includes camera means for sensing facial
15 characteristics of a user. The facial characteristics may be interocular separation or retina identification.

The secure access control system may allow for visual verification of the identity of a user to be made and in such an arrangement the key assembly data storage
20 means stores image data representative of an image of a user's face and the access control assembly includes image display means for displaying the image.

In another aspect this invention resides broadly in an operating system for a plurality of gaming machines,
25 the operating system including a secure access control system as defined in any one of the preceding statements wherein each gaming machine includes an access control assembly as described above. It is preferred that the access control assembly includes a user interface
30 assembly as described above.

As used herein the expression "gaming machine" includes any device, assembly or apparatus operable by a user for the purpose of entertainment and gambling. Examples of gaming machines include poker machines, slot
35 machines, pinball machines, roulette tables, blackjack machines, machines for playing bingo, lotto, jeuting and other similar lottery-type games, and TV sets and video screens programmed to facilitate gambling and the playing

of amusement games.

The gaming machines may be operable solely by coins and tokens in known manner, but it is preferred that the key assembly data storage means and the access control assembly data storage means each stores credit data representative of the credit held by a designated user. In such an arrangement it is further preferred that the credit data is incremented or decremented when a financial event associated with the key assembly is completed.

As used herein the expression "financial event" means any transaction which increases or decreases the credit held by a designated user of the operating system. Events which increment the credit data storage means include a cash deposit and a gaming machine win by a user, and events which decrement the credit data storage means include operation of a gaming machine by a user and operation of the user interface assembly to access a paging system to provide a chargeable service to the user.

In a preferred embodiment the operating system may include a paging system for transferring messages and paging signals from the gaming machines. In such an arrangement it is preferred that the user interface facility includes paging means whereby a user can access the paging system.

Gaming machines for use in the operating system of this invention may be custom-built for use therewith. However to enable older machines to be used in the operating system the gaming machines may include retrofit interface means for providing data transfer between an existing processor unit in an existing gaming machine and the access control assembly in the gaming machine. In the case of older machines which may not allow access to the processor unit the retrofit interface means may provide data transfer between photo-optic coin sensors, solenoid switches and motors in an existing machine and the access control assembly.

In a further aspect this invention resides broadly in a method of securing access, the method including:-

providing a key assembly having a data processing assembly including processor means and data storage means
5 for receiving identification data relevant to a user having authorised access;

inserting the key assembly in an access control assembly adapted to receive the key assembly and having a data processing assembly including processor means and
10 data storage means whereby communication is established between the access control assembly and the key assembly, and

verifying identification data stored in the key assembly data storage means.

15 In yet another aspect this invention resides broadly in a method of controlling the operation of a plurality of gaming machines linked to a central computer assembly by communication means for transferring data from the gaming machines to the central computer assembly, the
20 method including:-

providing users of the gaming machines with a key assembly having a data processing assembly including processor means and data storage means for receiving identification data relevant to a user and credit data
25 representative of the credit held by the user;

providing an access control assembly for each gaming machine, the access control assembly being adapted to receive the key assembly and having a data processing assembly including processor means and data storage means
30 whereby communication is established between the access control assembly and the key assembly, and

incrementing or decrementing the credit data when a financial event associated with the user is completed.

35 BRIEF DESCRIPTION OF THE DRAWINGS

In order that this invention may be more easily understood and put into practical effect, reference will now be made to the accompanying drawings which illustrate

a preferred embodiment of the invention, wherein:-

FIG 1 is a simplified schematic block diagram of a secure access control system including visual identification means;

5 FIG 2 is an illustration of a user interface assembly for use in the system of FIG 1;

FIG 3 is a flow diagram illustrating a photo identification process in the control system of FIGS 1 and 2;

10 FIG 4 is a detailed schematic block diagram of a secure access control system in accordance with the invention;

FIGS 5, 6 and 7 are schematic block diagrams of a secure access control system for a gaming establishment;

15 FIG 8 illustrates a player interface assembly for association with a gaming machine;

FIG 9 is a perspective view of a key assembly and housing therefor;

20 FIG 10 illustrates a player interface assembly attached to a poker machine;

FIG 11 is a flow diagram illustrating a machine playing sequence for a gaming machine connected in the control systems of FIGS 5, 6 and 7;

25 FIG 12 is a flow diagram illustrating a machine pay out sequence for a gaming machine connected in the control systems of FIGS 5, 6 and 7;

FIG 13 is a flow diagram illustrating entry of machine credit to a gaming machine connected in the control systems of FIGS 5, 6 and 7; and

30 FIG 14 is a flow diagram illustrating operation of a central crediting system connected in the control systems of FIGS 5, 6 and 7.

DETAILED DESCRIPTION OF THE INVENTION

35 A visual identification access control system in accordance with one embodiment of the present invention will now be described with reference to FIGS 1 to 3.

Visual identification access control system 11

comprises a visual sensor unit 12, an interface unit 13 arranged to interface with a key assembly memory storage device 14 and a processing means 15.

Control system 11 is connected to a secure system 5 16. The secure system is one which requires identification of a user before the user is allowed access to the system. Examples include automatic teller machines connected to central data base storing bank account information, and a control system where gaming 10 devices are connected to a central controller storing account information. The visual identification system of the present invention is not limited to use with these examples.

Each user of secure system 16 is provided with a key 15 assembly memory storage device 14 which contains image information relating to the visual facial appearance of the user. The memory storage device 14 may be an "intelligent key" containing a digital processing device and memory. The memory stores the image data in digital 20 form. The interface unit 13 includes an intelligent key reader which interfaces with memory storage device 14 to obtain the digital image data from the memory. The interface unit 13 provides the processor means 15 with the digital image information obtained from the memory 25 device 14.

The visual sensor unit 12 includes a camera 17 containing a charge coupled device (CCD) sensor and a lens positioned to view the face of a user standing by the apparatus. The CCD obtains a visual readout of the 30 facial appearance of the user and the sensor unit 12 converts this visual readout into digital form which is transmitted to the processor unit 15.

The processor unit 15 compares the digital image information obtained from the visual sensor unit 12 with 35 the digital information obtained from the interface unit 13. If the data from units 12 and 13 corresponds, processing means 15 determines that a positive identification has been made. That is, the person with

the key assembly memory device 14 is the same person being viewed through the lens. The processor 15 may then indicate to the secure system 16 that a positive identification has been made and the user will then be
5 allowed access to the secure system, eg to withdraw cash from a bank account.

Receiving means in the form of slot 18 is provided in unit 13 for insertion of intelligent key 14.

A keyboard 19 is also connected to the secure system
10 16. The keyboard may also be connected to the processor 15. The keyboard 19 allows a user to conduct transactions with the secure system 16. The number and type of keys provided on the keyboard 19 will depend on the functional requirements of the secure system 16.

15 FIG 2 shows a front view of the face 21 of user interface 13. (In this embodiment the keyboard 19 forms part of the interface unit 13.) A liquid crystal display 20 is provided for conveying information to the user. For example, the display may prompt the user to take
20 necessary action to progress the identification process.

In this embodiment the user is also provided with a PIN number which is entered by keyboard 22 before access to the secure system 16 is enabled. The use of both a PIN number and the visual identification technique
25 increases the security of the system.

In use, the display 20 can prompt the user to insert the key 14 into the slot 18. The user will then be asked to input the PIN number on the keyboard 22. If the PIN number is correct, the apparatus will proceed to the
30 visual identification stage. A switch 23 is provided to cause the camera 17 to be activated to take a frame. The switch 23 may be activated by the user. A frame is taken by the CCD unit, converted to digital and transferred to the processor unit 15. The lighting conditions at the
35 site are then altered (darker or lighter) and a second frame is taken by the CCD unit. A light sensor 24 is provided to detect lighting conditions. This frame is also converted to digital and transferred to the

processor unit 15. The change of light conditions ensures that the diameter of the pupil of the eye of the user will change. This is a test to ensure that the face is that of a real person and not a photograph. The processor will determine whether the pupil diameter has changed and if there has been no change, access to the secure system 16 will be denied. If pupil identification has changed the visual identification process will proceed.

10 The image stored in the key and obtained by interface unit 13 is transferred to the processor means 15. A comparison is then carried out between the image from the unit 12 and the image from the interface unit 13.

15 The flow chart of FIG 3 is illustrative of the above process.

FIG 4 is a detailed schematic block diagram of a secure access control system in accordance with the invention. A key assembly, user carriable device or memory storage device 25 includes data processing assembly 26 having a central processor or digital processing device 27 and data storage means 28 for storing identification data 29 and image data 30. Interface 31 provides communication between key assembly 25 and an access control assembly 33.

Access control assembly 33 includes a data processing assembly 44, user interface assembly or interface unit 45, receiving means 38 for receiving key assembly 25, and identity verification means 39.

30 Data processing assembly 44 is controlled by a central processor 34 and includes data storage means 35. User interface assembly 45 includes input means in the form of keypad 36 and information display means 37 in the form of a liquid crystal display as previously described. 35 Receiving means or keyslot 38 includes an interface 32 for providing communication with key assembly 25. Identity verification means 39 in the form of processor means adapted to compare information is associated with a

sensing means, sensor or visual sensing unit in the form of a camera 40 as previously described. Image display means 46 in the form of a video screen is provided at the access control assembly 33 to display a screen picture of the face of the legitimate holder of the key assembly 25. Interface means 41 is adapted to provide communication between access control assembly 33 and other access control assemblies and a central computer assembly or control unit 42 via communication bus 43.

10 A gaming establishment control system which incorporates an operating system in accordance with an embodiment of the present invention will now be described with reference to FIGS 5 to 14.

With reference to FIGS 5 and 6, the control system comprises a central computer 42 for controlling operations of the system. A communication system generally designated by reference numeral 43 connects the central computer 42 to peripheral units. A plurality of gaming machines 49 are connected to the control system. 15 Poker machines incorporate counters 54 for counting the number of credits input to a machine and taken out of the machine during a predetermined playing period and for monitoring sundry other machine operations, switches 55 controlled by a keyboard for operation of the machine and 20 coin in/out meters 56 which provide a number of pulses when coins are input or taken out of the machine. Conventional poker machines are coin operated and prizes may be paid out in coins at the machine. This embodiment of the present invention enables operation of poker 25 machines without the need to insert coins. Further, no coin pay out is necessary when a prize is won.

A large gaming establishment may have many hundreds of poker machines. All these poker machines may be connected in the control system of the present embodiment of the invention. The control system includes an access control assembly 57 associated with each poker machine 35 49. Each access control assembly 57 is connected in a loop format in which each assembly for each poker machine

is connected. The loop is connected to the central computer 42. Serial data lines are used for the loop communication system. Two serial data communication lines are employed, one for carrying data and the other
5 being supervisory. Depending on how many machines 49 are to be connected in the control system, a plurality of loops may be employed.

The control system also incorporates a number of other types of terminals, apart from the gaming device
10 access control assemblies 57, which are also connected to the central computer by the communication system 43. These include remote cash register units 58, remote auto-teller units 59, and credit/debit terminals 60.

The central computer 42 is also connected to a
15 paging system 52 having CPU control unit 61 and paging transmitter 62. These provide a paging service. The computer is also connected to computer controlled signs 63, which may be for the purpose of advertising, providing linked jackpot information etc.

20 The system constitutes a complete control system for monitoring operation of the gaming establishment. Transactions with each machine 49 can be monitored by the central computer 42. In addition, financial transactions at other points in the establishment, such as at the bar
25 or restaurant, can also be monitored by the central computer. The paging function enables services to be provided to users of the machine 49 without the users needing to leave their seat by the machine. Keyboard means such as keys 53 as described with reference to FIGS
30 7 and 8 and associated with the access control assembly 57 are actuable to instigate a paging function to call a service operator to attend to the needs of the user, depending upon the key actuated on the user assembly 45.

Gaming machines for use in the operating system of
35 this invention may be custom-built for use therewith. As seen in FIGS 6 and 7, to enable older machines to be used in the operating system the gaming machines 49 have a retrofit interface board 50 which includes adaptor

circuits specific to a given machine for providing data transfer between an existing processor unit and access control assembly 57. Some older machines do not allow access to the processor unit and interface board 50 provides data transfer between photo-optic coin sensors, solenoid switches and motors and access control assembly 57.

FIG 8 illustrates a user interface unit 64 to be mounted on each machine 49 as shown in FIG 10. The unit 64 is operable by the user on insertion into the key slot 65 of an intelligent key 25 containing a micro processor and memory store. Key slot 65, which with key 25 is illustrated in perspective view in FIG 9, is installed in user interface unit 64 with an upwards inclination so that the drinks of users if accidentally spilled, will not collect in the slot. It will of course be realised that the interface unit may be built into the gaming machine and that in the case of video machines, the display means can be the video screen.

To obtain access to the machine 49, the user inserts intelligent key 25 into the key slot 65 and enters the PIN number by actuation of the appropriate keys on the keyboard 66. The intelligent key 25 contains in its memory credit information indicating the amount of credit available to the owner of the key for playing the machines 49. Whether the player has enough credit on the key will be checked by the unit 64 and if approved the player will be allowed to play machine 49. The player may play the machine with any amount of credit available on the key 25. As credit is entered to play the machine it is debited from the key 25. Winnings are credited to the memory store on the key.

The control system will also "double check" the credit on the key with account information for the user held on data base by the central computer 42. This check is preferably carried out before play commences. If there is an inconsistency between the account on central data base and the credit shown on the key, the user will

be asked to report to an office of the gaming establishment and will not be allowed to play the machine.

The user's account on the central computer 42 may
5 also be updated in response to playing the gaming machine
49. If a user's account or key has no credit, credit may
be obtained at a change box having debit/credit unit 60.
If the user deposits money at the change box it will be
credited to both key and account by the debit/credit unit
10 60. The player can then proceed to play a machine.

The central computer 42 may also obtain other
transaction information from the machines 49. Any
information required for audit purposes may be obtained
by the central computer 42 in this manner. There is no
15 need for an operator to physically attend a machine
except in cases of malfunction. The central computer 42
continually polls the machines for data.

If a user requires a service function or a drink at
the machine, the appropriate button 53 on the keyboard is
20 pressed and a service operator will be paged by the
paging system. The central computer 42 detects that a
paging operation is required and causes the paging CPU 61
to cause a paging transmission via paging transmitter 62
to page a designated operator by a remote paging unit.
25 The designated operator can then approach the user to
carry out the required service. If a drink or other
service is to be provided which will cost the user money,
the user may pay for it by debiting credits from his key.
This can be done at the user interface unit 64.

30 Any number of desired paging functions can be
carried out by the paging CPU 61. The paging system is
responsive not only to users, and a facility is provided
for automatically paging service operators in some
circumstances.

35 For example, if a key is accidentally left in
machine 49 after a predetermined time the service
operators are paged with an appropriate message. If
credits are accidentally left on a machine the attendant

will again be paged with an appropriate message after the elapse of a given time without machine activity. The attendant can then clear the machine by inserting an operator key and entering a code. The computer 42 will
5 be updated with the member's new credit. This will cause a discrepancy between the member's key and the credit in the central computer, and the next time the member plays a machine the display 37 will signal to the member to check at the change box. The key credit can then be
10 updated by the cashier.

In order to obtain cash the user utilises a change box or reception 60. Money can be collected from the change box and the key credit will be debited.

Key reader units 58 are provided at the bar,
15 restaurant and at other locations to enable a user to use a key to obtain other services. These units are also connected to the central computer 42 to update account information.

Auto-teller units 59 are also provided and may have
20 a facility for visual identification in accordance with the first aspect of the present invention.

FIG 7 is a detailed schematic block diagram of an operating system for a number of gaming machines 49 utilising a secure access control system 57 in accordance
25 with the invention. A key assembly, user carriable device or memory storage device 25 includes data processing assembly 26 having a central processor or digital processing device 27 and data storage means 28 for storing identification data 29, image data 30 and
30 credit data 47. Interface 31 provides communication between key assembly 25 and access control assembly 57.

Access control assembly 57 includes a data processing assembly 44, user interface assembly or interface unit 45, receiving means 38 for receiving key
35 assembly 25, and identity verification means 39. Access control assembly 57 can be connected to a gaming function 51 by a retrofit interface unit 50 as previously described.

Data processing assembly 44 is controlled by a central processor 34 and includes data storage means 35 for storing credit data 47 and gaming machine data 48. A user interface assembly 45 includes input means in the form of keypad 36, information display means 37 in the form of a liquid crystal display and paging means or buttons 53 as previously described. Receiving means or keyslot 38 includes an interface 32 for providing communication with key assembly 25. Identity verification means 39 in the form of processor means is adapted to compare information. Interface means 41 is adapted to provide communication between access control assembly 33 and communication bus 43 for communication with other access control assemblies and a central computer assembly or control unit 42 and to a paging system 52.

It will be realised that a cashless system can be provided in accordance with the invention in which the intelligent key contains an electronic photo ID facility, key number, user function (member, attendant, operator), user details (name, address) and transaction details.

The key holder has a PIN code which is not accessible to operators. Transactions are stored and reported by key number and not by member name. The key can be used for different clubs with the data of one club not being accessible by other clubs. The key is thus extremely secure and cannot be copied.

Key readers are provided on each machine, at each entrance with monitors for photo ID check, at each payout area optionally with an ID monitor, at each bar service area, at reception area with camera for new membership, and at automatic tellers with reader/writer/camera.

FIGS 11 to 14 are self-explanatory flow charts showing machine playing sequence, machine pay out sequence, entry of credit into the machine and operation of the central crediting system. The following brief summaries outline operation of the system in a club or casino and should be read in conjunction with FIGS 11 to

14.

Credit System:-

- . Member pays for credits at change box.
- . Member key inserted in reader, enters PIN number.
- 5 . Operator checks details and enters credit amount.
- . Credit placed on key and key ejected.
- . Transaction with member, operator, amount, date logged on CPU.

Machine Player System:-

- 10 . Insert key in machine.
- . Display asks for PIN number.
- . Enter PIN number.
- . Main CPU checks details and credit.
- . Display asks for amount required to be entered in
- 15 machine.
- . Enter amount.
- . Credit on key and CPU are updated.
- . Key removed.
- . Coin credit meter on machine incremented.
- 20 . When play finished insert key in reader and press "collect" on poker machine.
- . Key and CPU updated with credits and machine coin credits cancelled.
- . Remove key.
- 25 . If a key is accidentally left in a machine after a predetermined time the attendants are paged with a message indicating a key may be left in the machine.
- . If there are no credits left on the machine at the end of play there is no need to insert the key - the
- 30 machine will automatically be released after predetermined time.
- . A member may reserve a machine, with credits on it, and without having his key actually in the machine, and get a drink etc - the machine will not accept
- 35 any other key (except an attendants) when in this mode.
- . If credits are accidentally left on a machine the attendant will again be paged with an appropriate

message after a time without machine activity. The attendant can then clear the machine by inserting his key and entering a code. The CPU will be updated with the members new credit. This will give a discrepancy between the member's key credit and the credit in the CPU. The next time the member plays a machine he will be asked by the display to check his credits at the change box. The key credit will then be updated by the cashier (a message with the reason for the update will be given at their terminal).

Payout:-

- . Money collected from key credit at change box, automatic teller.
- . Key inserted in reader.
- . PIN number entered.
- . Credit amount checked by CPU
- . Photo ID if required.
- . OK given to operator.
- . Record again kept of transaction

Machine Attendants:-

- . Attendants have their own keys.
- . Log on/off duty can be performed.
- . Key inserted in machine before any service.

25 Reports:-

Reports can be generated by management by selecting their own set of specifications from the database.

Examples include:-

- | | | |
|----|-----------------|--------------------------------|
| 30 | Cash in | - from credits entered to keys |
| | Cash out | - from key credits cashed in |
| | Key Credits | - credit on keys not claimed |
| | Bar Cash | - key credits used at bar |
| | | - cash taken at bar |
| | Meter Readings | - all functions |
| 35 | Player Activity | - types of players, machines, |
| | Restaurant Cash | - cash credits used |
| | | - cash taken |
| | Entertainment | - key credits used |

- cash taken

It will be appreciated that a secure access control system in accordance with the present invention has many advantages.

5 The provision of a secure intelligent user key, on-site processor storage capacity and the ability to check identity on site without the necessity to revert to a central computer, enables stand-alone operation and means there is little restriction on the number of sites which
10 can be run on a single extended network. Integration of an internal paging system enables automatic reporting on all important events within the system to users who are potentially concerned with an event, and provides extremely efficient utilisation of human resources.
15 Furthermore, it offers immediate service to customers and users in casino-type installations.

 The system allows for both supervisory control and data transfer whereby multiple facilities can be provided with minimum congestion. Electronic signs such as
20 general information, jackpot information and advertising can be easily controlled and it is possible with the system to provide inter-establishment jackpots as well as internal jackpots.

 The secured access control system in accordance with
25 this invention also provides a facility for central updating whilst monitoring all sites, and generates virtually real time information from all sites.

 The paging facilities provide automatic ordering of goods on site, jackpot information for management,
30 machine reserve reporting and indicates to staff the need to service machines. These capabilities provide significant advantages in clubs, casinos and the like.

 It will be realised that a central computer failure does not cause the system to fail and that individual
35 operations can continue on-site because of the provision of on-site processor facilities and the high level security provided by the intelligent card. The central computer is updated when it comes back on-line.

Linked jackpot facilities can only be provided satisfactorily with on-line systems and the utilisation of linked jackpots is facilitated by the present invention because of the instant automatic paging facilities which are available if problems occur. Provision of such a system is desirable for the smooth operation of linked jackpots.

It will also be realised that the system according to the present invention overcomes certain problems of the prior art and in particular provides for the automatic update of player records and so does not rely on a player having to hand in a key in order for the centralised computer to access information for collation and analysis. This is one disadvantage with the system outlined in Australian patent application 72657/91 because of the fact that it is usual for players at casinos to lose their credit and there is thus often little incentive for a player to return a key to a central location.

Furthermore, by providing a system in which individual debits are incremented each time a machine is played, the system of this invention overcomes disadvantages of earlier "cashless" systems in which the total amount of credit is downloaded into the machine when the player's card is inserted in the machine and read by the card reader. This is of particular significance if, as is usual, regulatory authorities require an electro-mechanical counter to be maintained in machines even if operation is controlled by a CPU. The downloading of a large number of credits, for example when a relatively large cash deposit is made when a card is inserted into a small value machine, means that such a counter can fail due to excessive mechanical wear or the machine is either ineffective or substantially inoperable for the time taken for the machine to increment the total number of credits.

Furthermore, intelligent processors in known systems do not contain player credit information and it is

necessary that the player's card be accessed in order to obtain such information. Security is thereby compromised because the card and the machine do not both contain updated credit records and the card itself can be
5 subjected to electronic tampering.

The invention thus provides a practical "cashless" casino operating system which is able to support a very large number of gaming machines without the need to provide a high powered and expensive central computer
10 system.

It will of course be realised that whilst the above has been given by way of an illustrative example of this invention, all such and other modifications and variations hereto, as would be apparent to persons
15 skilled in the art, are deemed to fall within the broad scope and ambit of this invention as is hereinafter claimed.

CLAIMS

1. A secure access control system including:-
at least one key assembly having a data processing
5 assembly including processor means and data storage means
for receiving identification data relevant to a user of
said system;
a plurality of access control assemblies adapted to
receive a key assembly, each said access control assembly
10 having a data processing assembly including processor
means and data storage means, and
interface means whereby an access control assembly
can communicate with a received key assembly.
- 15 2. A secure access control system as claimed in claim
1, wherein each said access control assembly includes a
user interface assembly operable by a user to input data
to said access control assembly.
- 20 3. A secure access control system as claimed in claim
2, wherein said user interface assembly includes input
means and information display means.
4. A secure access control system as claimed in claim
25 3, wherein said input means includes a keypad.
5. A secure access control system as claimed in claim
2, wherein said access control assembly includes
receiving means for closely receiving and releasably
30 retaining a said key assembly whereby communication is
established between said access control assembly and said
key assembly by said interface means.
6. A secure access control system as claimed in claim 1
35 or claim 2, wherein each said access control assembly has
identity verification means for verifying identification
data stored in said key assembly data storage means.

7. A secure access control system as claimed in claim 6, wherein said identity verification means includes sensing means for sensing personal characteristics of a user.

5

8. A secure access control system as claimed in claim 7, wherein said sensing means includes camera means for sensing facial characteristics of a user.

10

9. A secure access control system as claimed in claim 1, wherein said key assembly data storage means stores image data representative of an image of a user's face and said access control assembly includes image display means for displaying said image.

15

10. An operating system for a plurality of gaming machines, said operating system including a secure access control system as defined in any one of the preceding claims, wherein each said gaming machine includes an access control assembly.

20

11. An operating system for a plurality of gaming machines as claimed in claim 10, wherein said access control assembly is as defined in claim 2.

25

12. An operating system for a plurality of gaming machines as claimed in claim 11, wherein said key assembly data storage means and said access control assembly data storage means stores credit data representative of the credit held by a designated user.

30

13. An operating system for a plurality of gaming machines as claimed in claim 11, wherein said credit data is incremented or decremented when a financial event associated with said key assembly is completed.

35

14. An operating system for a plurality of gaming machines as claimed in claim 11, and including a paging

system for transferring messages and paging signals from said gaming machines.

15. An operating system for a plurality of gaming machines as claimed in claim 14, wherein said user interface facility includes paging means whereby a user can access said paging system.

16. An operating system for a plurality of gaming machines as claimed in claim 10, wherein said gaming machines include retrofit interface means for providing data transfer between a processor unit in an existing gaming machine, or between photo-optic coin sensors, solenoid switches and motors in an existing machine, and the access control assembly in said gaming machine.

17. A method of securing access, said method including:-
providing a key assembly having a data processing assembly including processor means and data storage means for receiving identification data relevant to a user having authorised access;

inserting said key assembly in an access control assembly adapted to receive said key assembly and having a data processing assembly including processor means and data storage means whereby communication is established between said access control assembly and said key assembly, and

verifying identification data stored in said key assembly data storage means.

30

18. A method of controlling the operation of a plurality of gaming machines linked to a central computer assembly by communication means for transferring data from said gaming machines to said central computer assembly, said method including:-

providing users of said gaming machines with a key assembly having a data processing assembly including processor means and data storage means for receiving

identification data relevant to a user and credit data representative of the credit held by said user;

providing an access control assembly for each said gaming machine, said access control assembly being
5 adapted to receive said key assembly and having a data processing assembly including processor means and data storage means whereby communication is established between said access control assembly and said key assembly, and

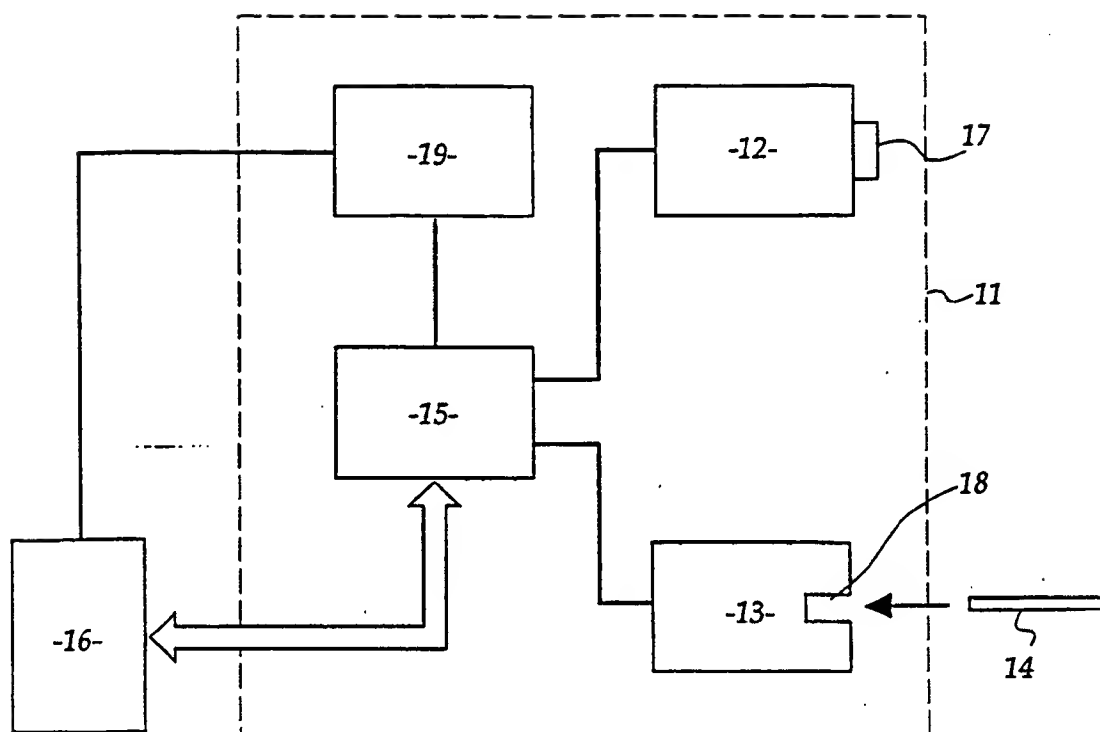
10 incrementing or decrementing said credit data when a financial event associated with said user is completed.

19. A secure access control system as claimed in claim 1, said control system including:-

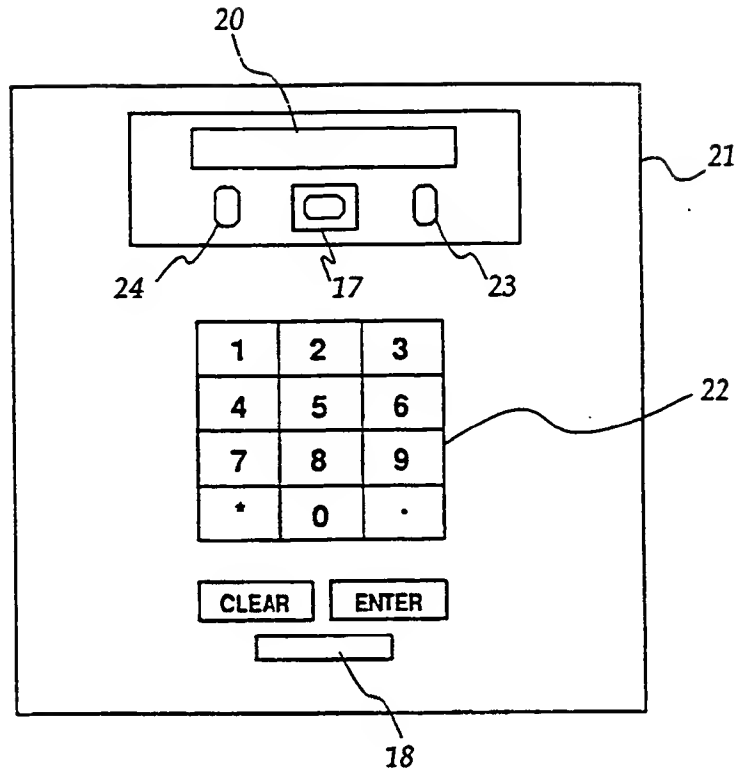
15 a central computer assembly, and

communication means for transferring data from said access control assemblies to said central computer assembly.

1/13

*Figure 1.*

2/13

*Figure 2.*

3/13

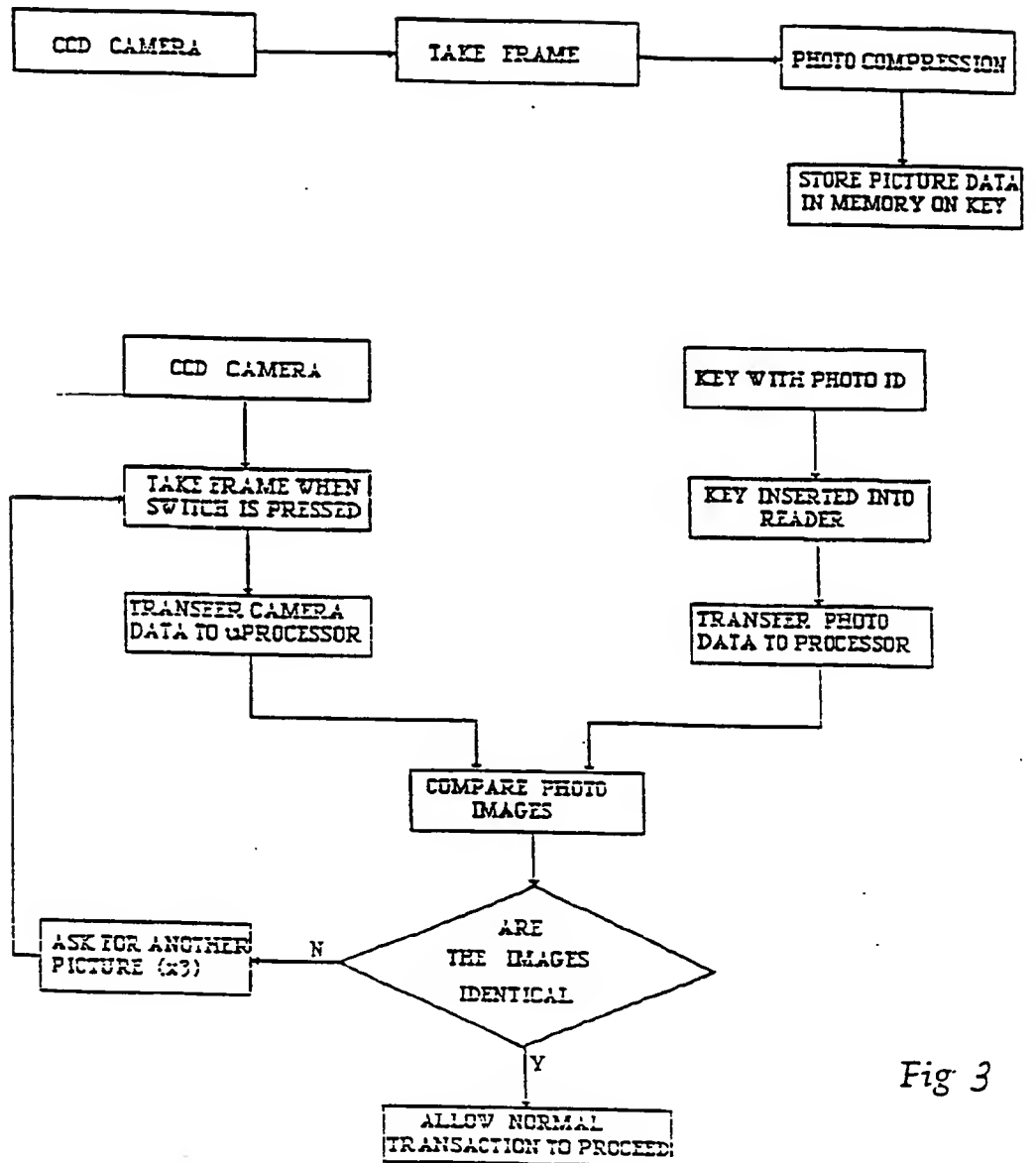


Fig 3

SUBSTITUTE SHEET

4/13

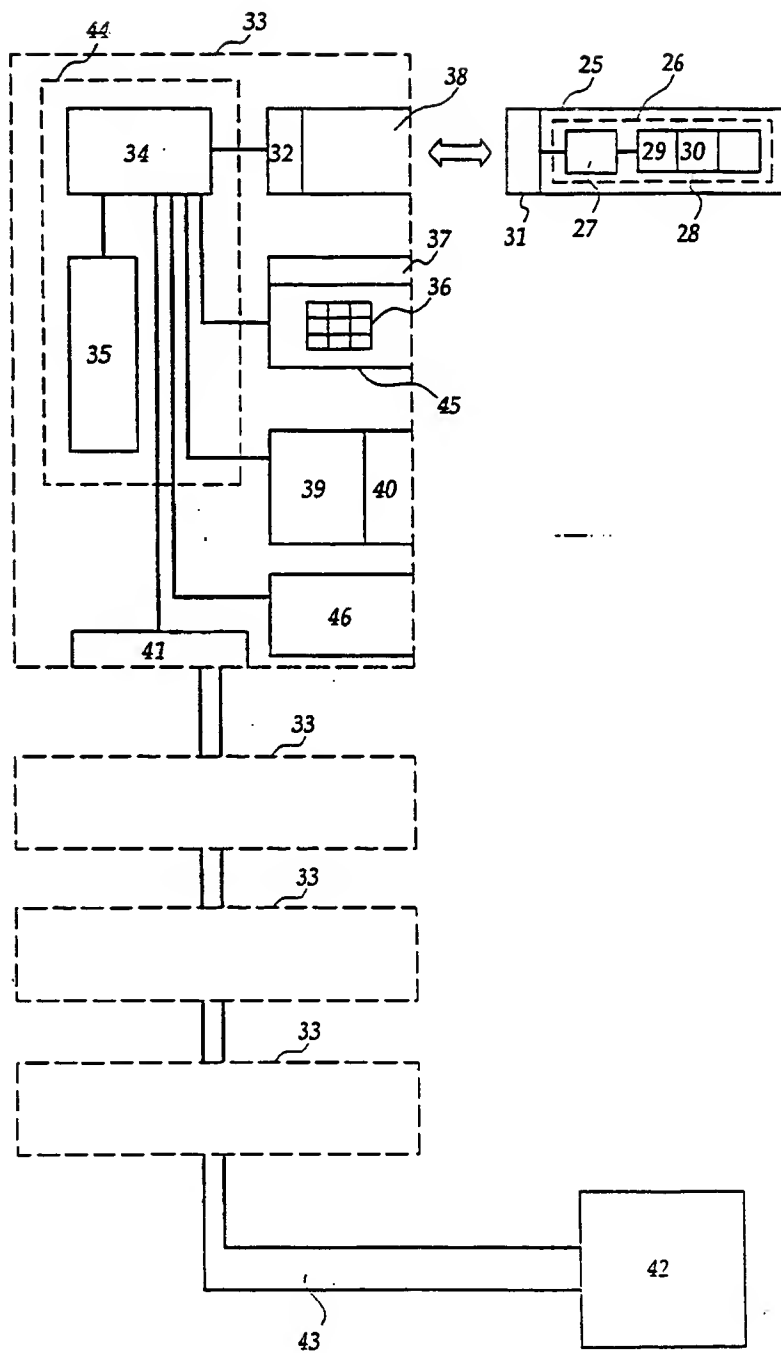


Figure 4.

5/13

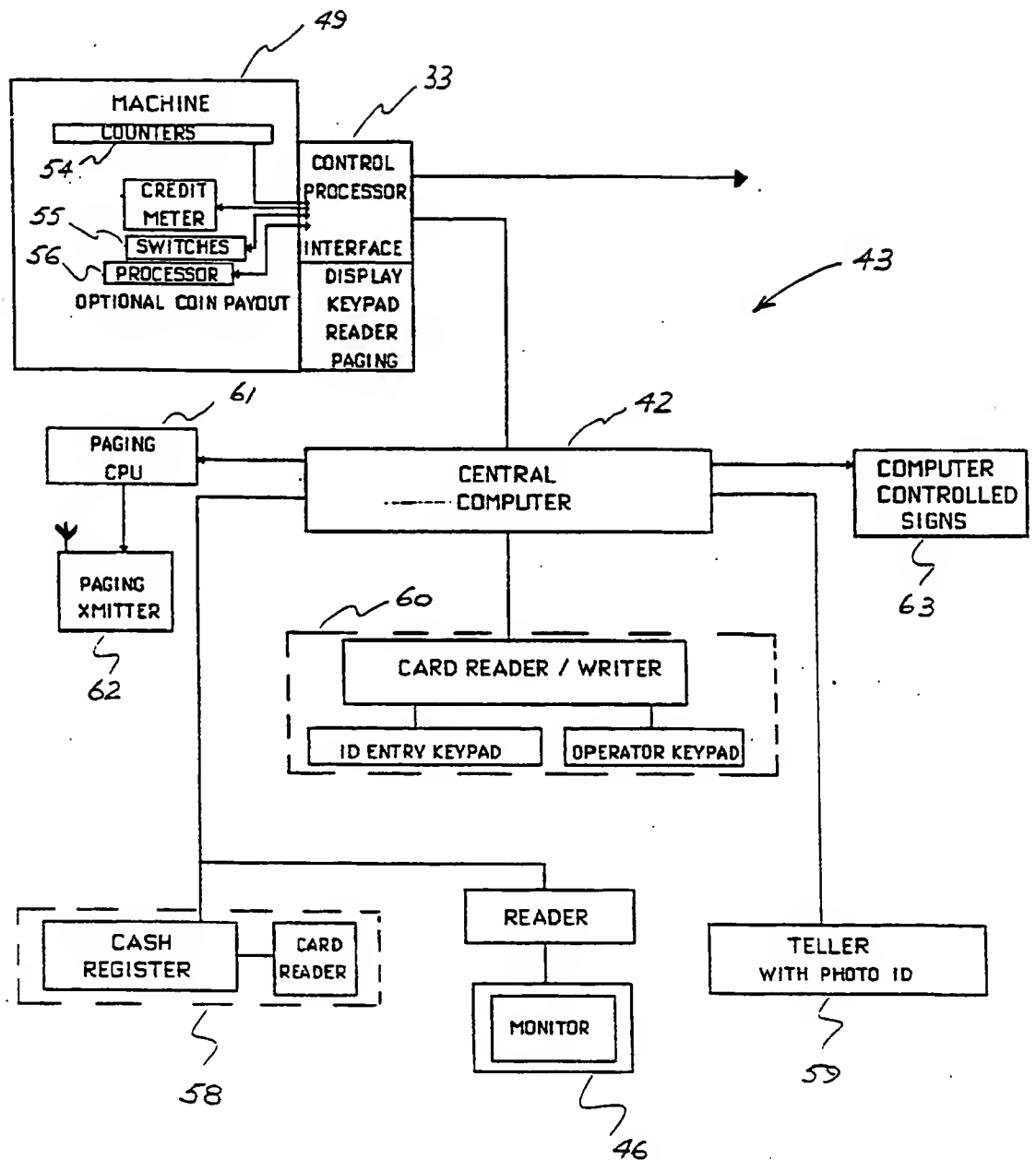


Fig 5

6/13

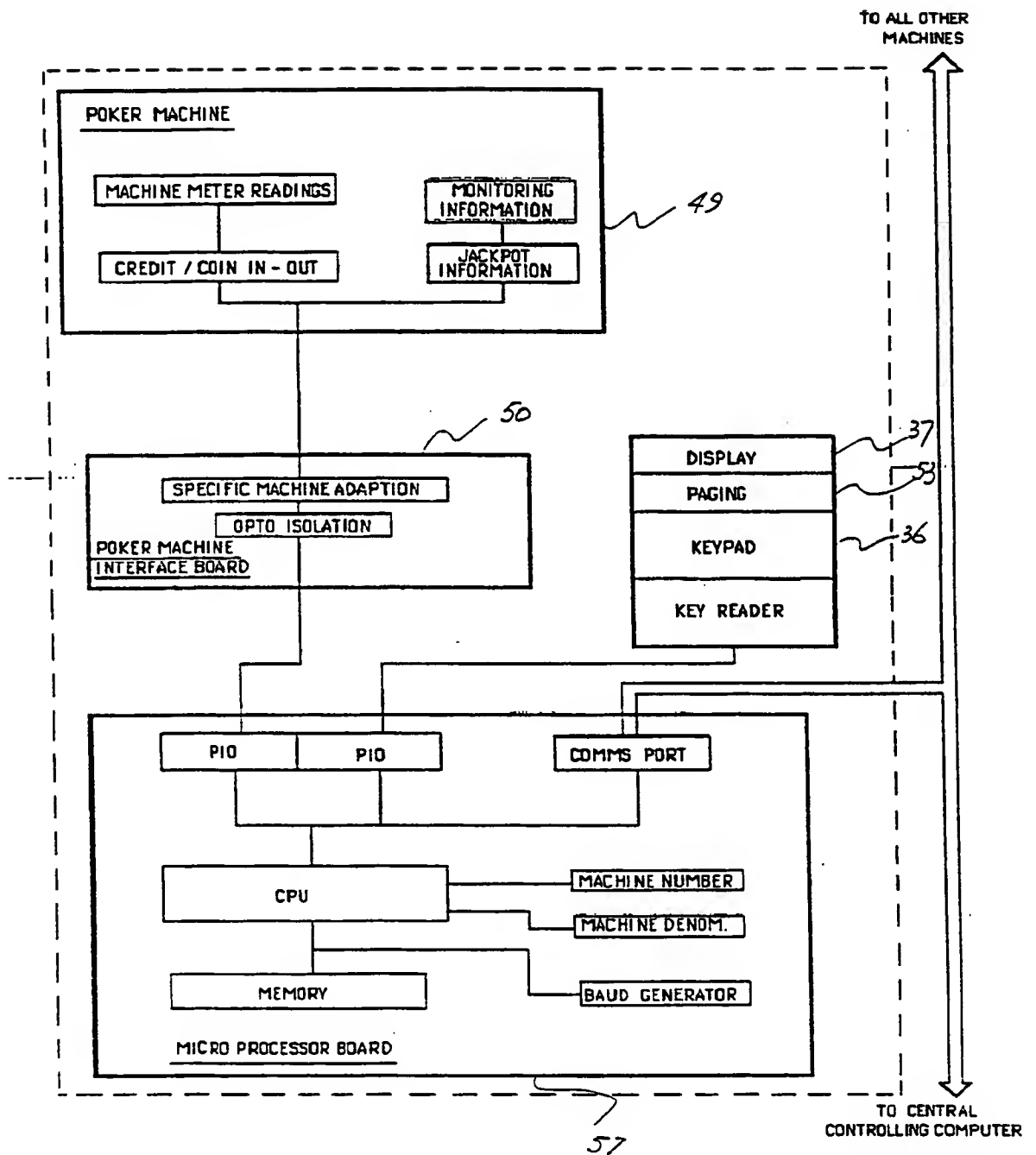


Fig 6

7/13

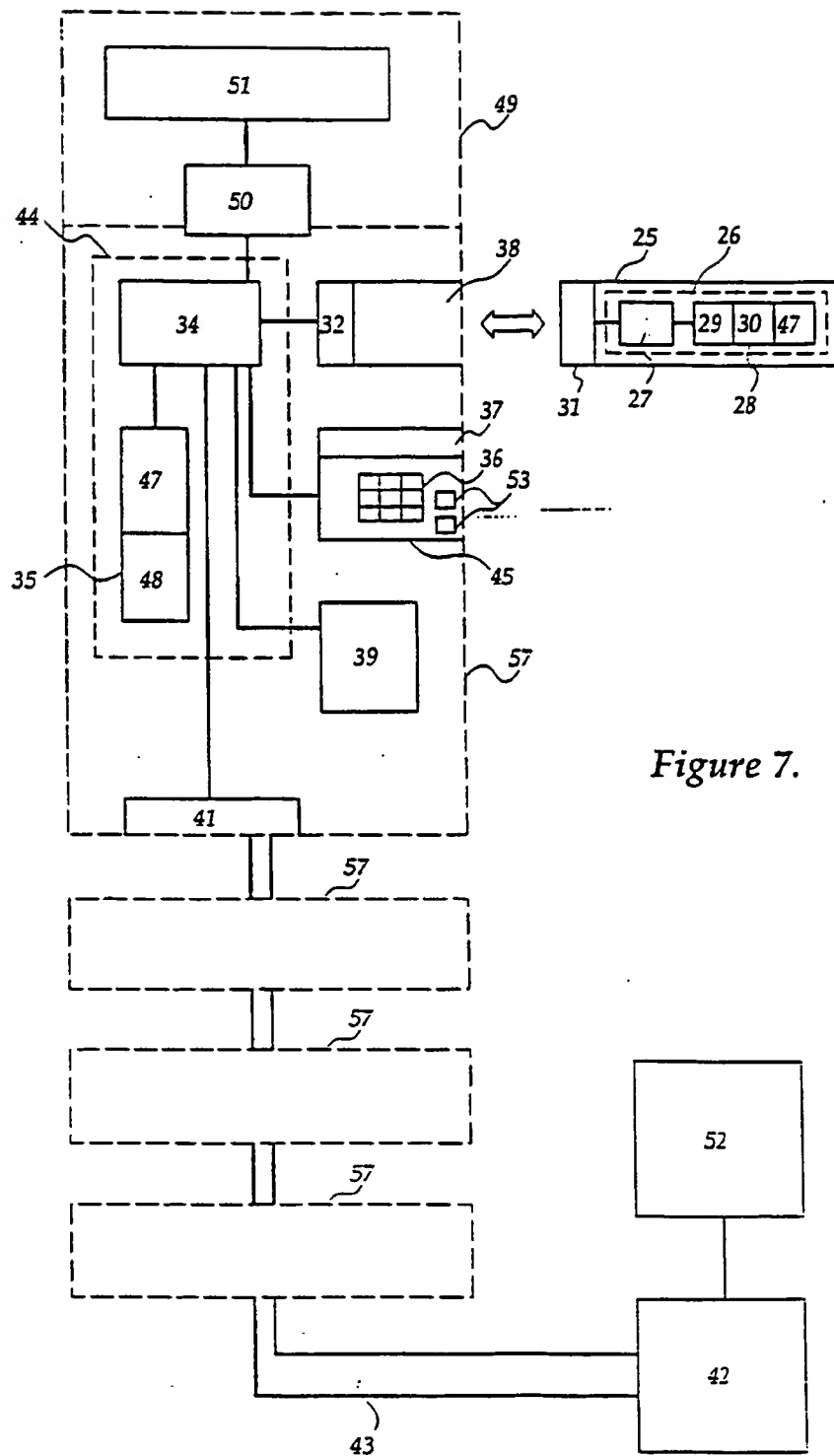


Figure 7.

8/13

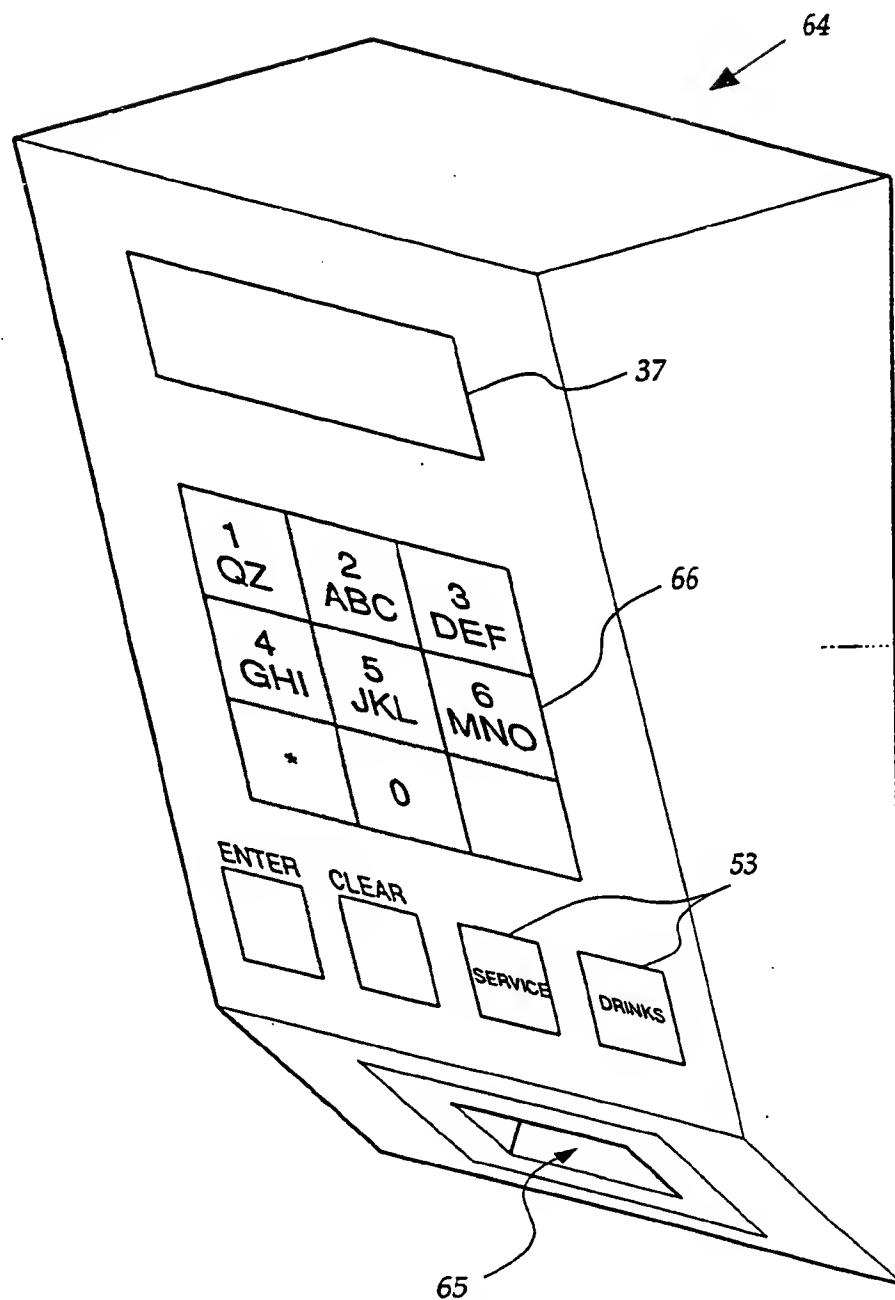


Figure 8.

9/13

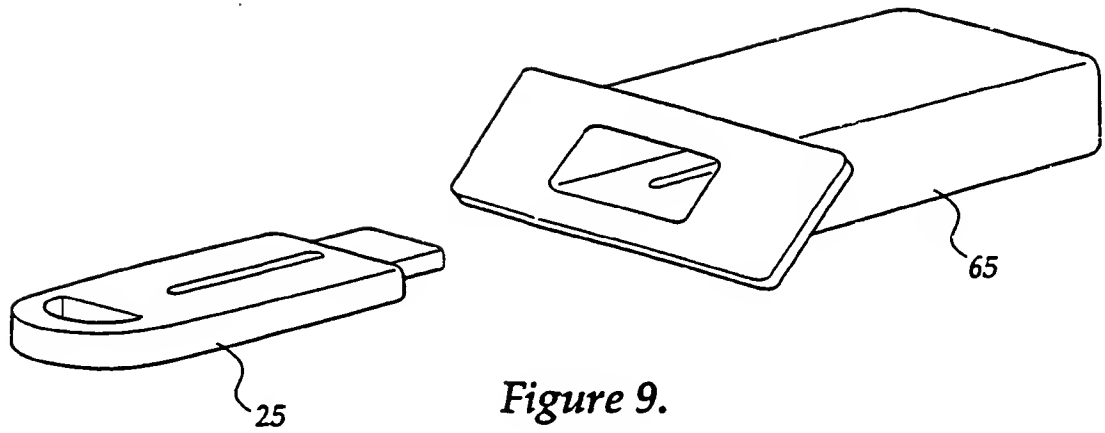


Figure 9.

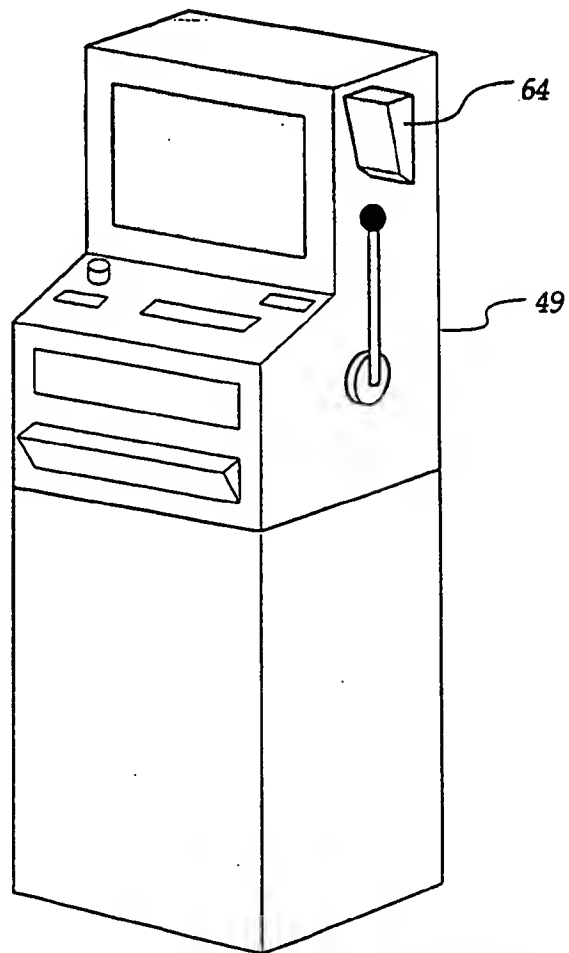


Figure 10.

10/13

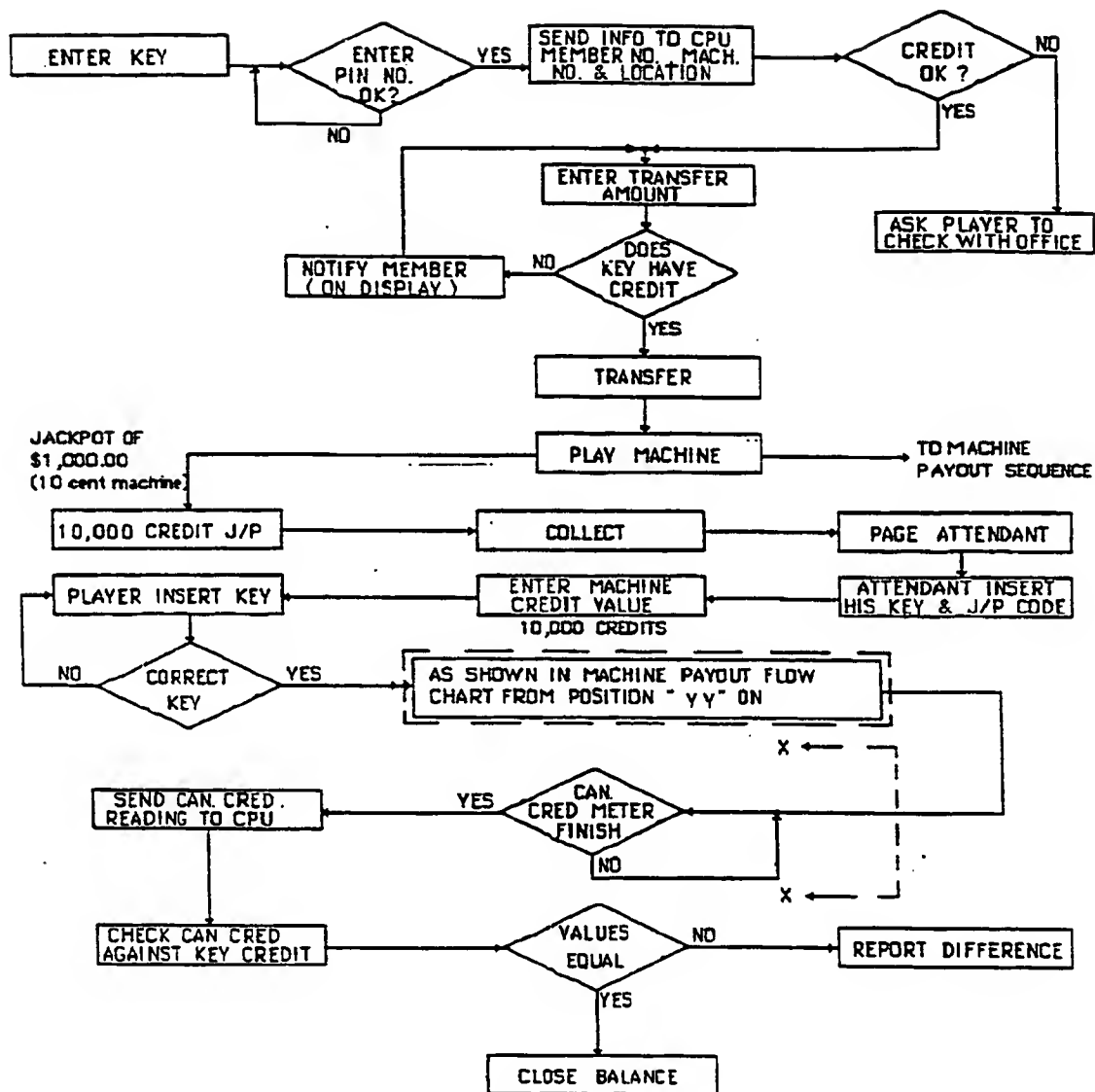


Fig 11

SUBSTITUTE SHEET

11/13

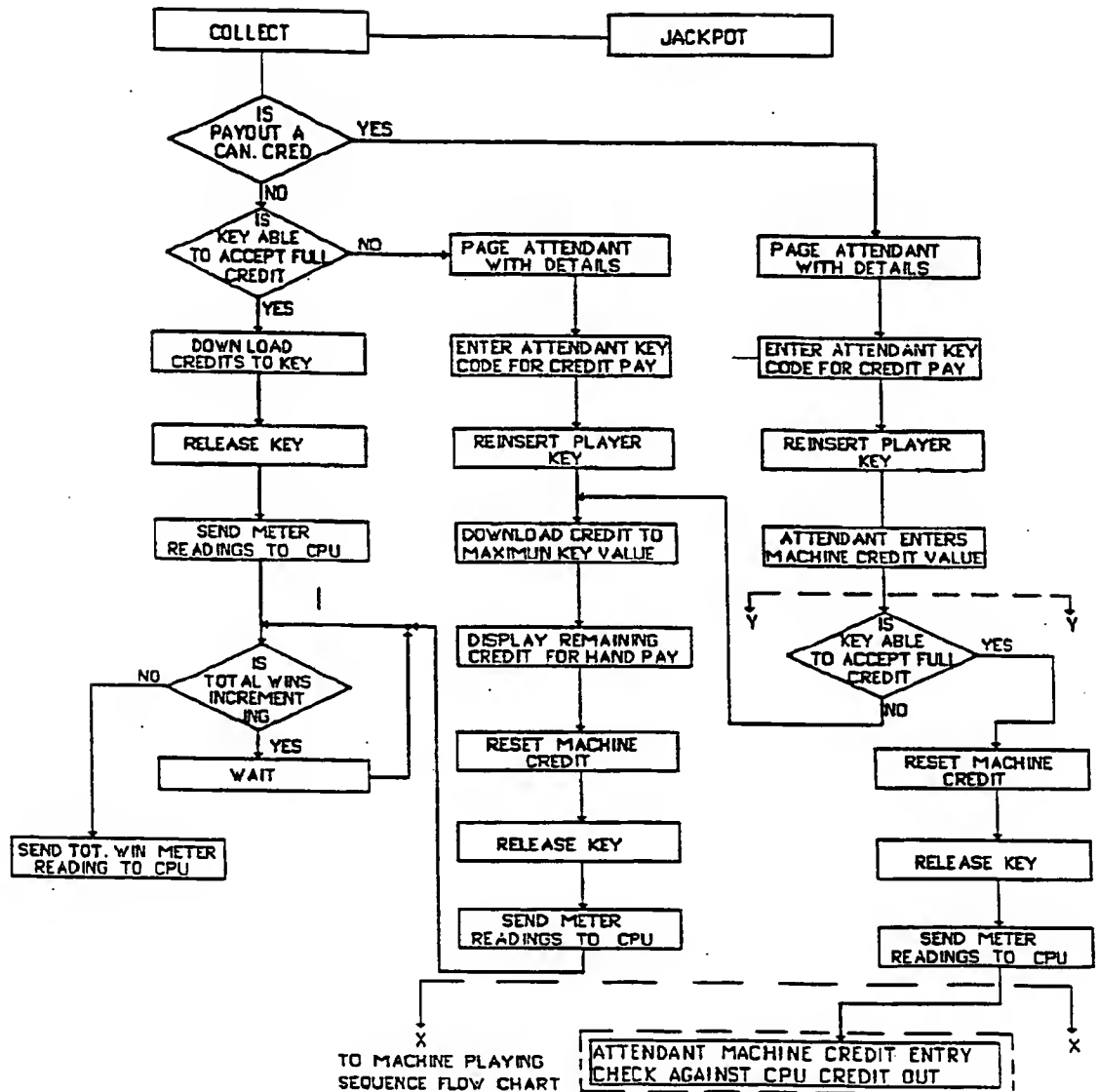


Fig 12

12/13

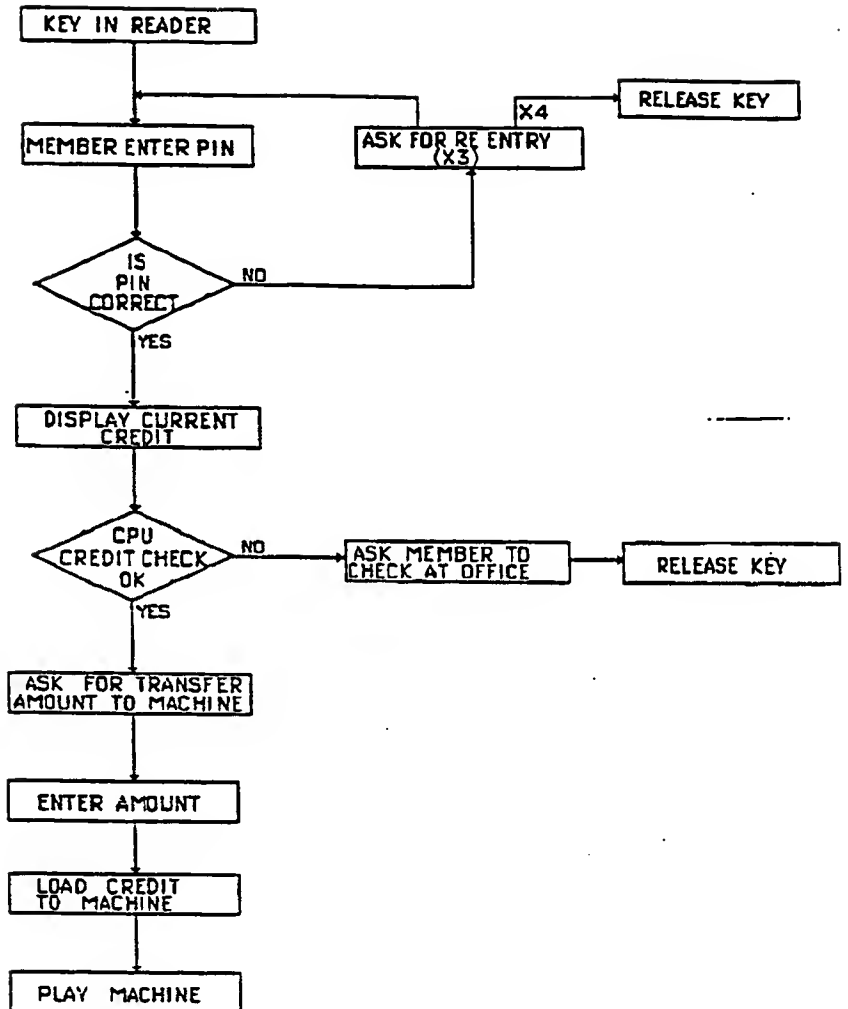


Fig 13

13/13

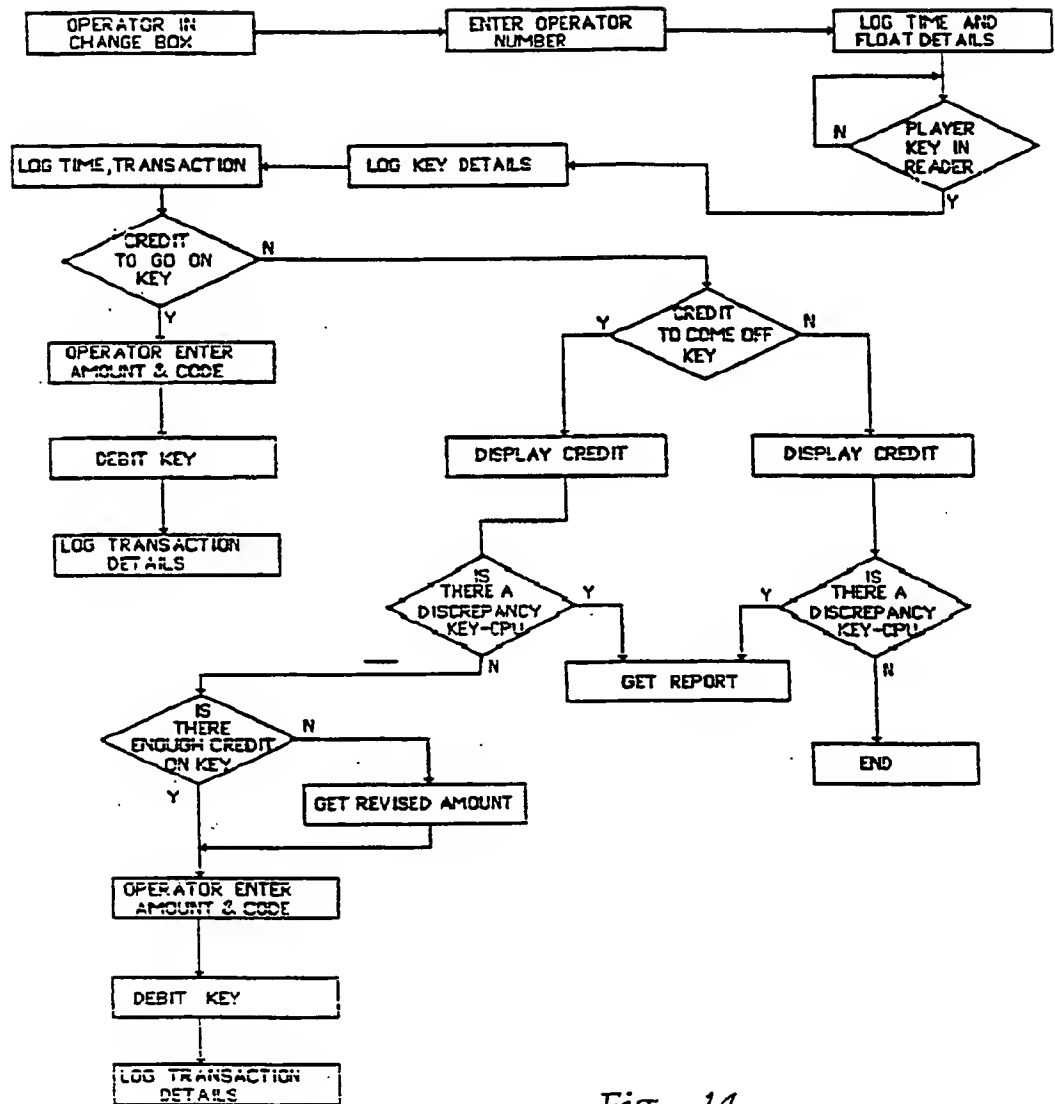



Fig 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU 93/00576

A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. ⁵ G07C 9/00, G07F 7/10 According to International Patent Classification (IPC) or to both national classification and IPC					
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC G07C 9/00, G07F 5/18, 7/10, 7/12 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched AU : IPC as above Electronic data base consulted during the international search (name of data base, and where practicable, search terms used)					
C. DOCUMENTS CONSIDERED TO BE RELEVANT					
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.			
X Y	AU,A, 25291/92 (BALLY MANUFACTURING CORPORATION) 25 March 1993 (25.03.93)	1-6,10-19 7,8			
X Y	US,A, 4764666 (BERGERON) 16 August 1988 (16.08.88) <div style="text-align: center;">(continued)</div>	1-6,10-13,17-19 7,8			
<div style="display: flex; justify-content: space-between;"> <input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex. </div>					
<table style="width: 100%; border: none;"> <tr> <td style="width: 33%; vertical-align: top;"> * Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed </td> <td style="width: 33%; vertical-align: top;"> "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family </td> <td style="width: 33%;"></td> </tr> </table>			* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family	
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family				
Date of the actual completion of the international search 3 February 1994 (03.02.94)		Date of mailing of the international search report 17 FEB 1994 (17.02.94)			
Name and mailing address of the ISA/AU AUSTRALIAN INDUSTRIAL PROPERTY ORGANISATION PO BOX 200 WODEN ACT 2606 AUSTRALIA Facsimile No. 06 2853929		Authorized officer <div style="text-align: center;">  R. TOLHURST Telephone No. (06) 2832187 </div>			

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU 93/00576

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate of the relevant passages	Relevant to Claim No.
X	US,A, 4800520 (IJIIMA) 24 January 1989 (24.01.89)	1-6,17,19
Y		7,8
Y	AU,A, 72657/91 (QUIGG) 12 September 1991 (12.09.91)	1,2,5,10-13,16,17
X	WO,A, 87/07063 (AMERICAN TELEPHONE & TELEGRAPH COMPANY) 19 November 1987 (19.11.87)	1,2,5,16,17,19
Y		7,8
X	EP,A, 182244 (OKI ELECTRIC INDUSTRY COMPANY LTD) 28 May 1986 (28.05.86)	1-6,17
Y		7,8
X	EP,A, 504616 (ASCOM AUTELCA AG) 23 September 1992 (23.09.92)	1-7
Y		8
Y	WO,A, 86/05018 (FLOM & SAFIR) 26 August 1986 (26.08.86)	7,8
A,P	EP,A, 531241 (HELLO S.A.) 10 March 1993 (10.03.93)	
A	AU,A, 70780/91 (LUCERO) 18 July 1991 (18.07.91)	
A	AU,A, 11056/88 (COUNTRYWIDE COMPETITIONS LIMITED) 1 August 1989 (01.08.89)	
A	AU,B, 32715/78 (511904) (BELL-FRUIT MANUFACTURING COMPANY LIMITED) 2 August 1979 (02.08.79)	

INTERNATIONAL SEARCH REPORT
information on patent family members

International application No.

PCT/

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report				Patent Family Member			
AU	25291/92	CA	2078936	EP	534718		
US	4764666	AT	85142	AU	22186/88	CA	1294052
		DE	3877868	EP	307925	ES	2037168
		JP	1222374	US	4764666		
US	4800520	DE	3636700	FR	2591780	JP	62102385
		KR	9002070				
WO	8707063	AT	77707	CA	1287920	DE	3780008
		EP	270571	JP	1500378	KR	9208755
EP	182244	DE	3576009	EP	182244	JP	61114895
		KR	9208069	US	4864109		
WO	8605018	AT	65851	BR	8605561	CA	1244552
		DE	3680618	EP	215818	IL	77920
		JP	62501889	MX	163339	US	4641349
EP	531241	CA	2077361	FR	2680901	US	5278395
AU	70780/91	CA	2016452	EP	506873	NZ	236562
		US	5038022	WO	9109369		
AU	11056/88	WO	8906405				
AU	32715/78	AU	32714/78	CA	1112766	CA	1114065
		DE	2803214	DE	2803215	ES	466313
		ES	466314	GB	1558521	IE	46312
		IE	46313	NL	7800837	NL	7800838
END OF ANNEX							